Cryptography: Symmetric encryption

Instructor: Sarada Prasad Gochhayat
Office: ECSB 1310
Phone:
E-mail: sgochhay@odu.edu

Lectures: Wednesday, 7:10 pm – 9:50 pm
Textbook: Internet Security, A Hands-on Approach, Wenliang Du
Class webpage: www.blackboard.odu.edu

COURSE DESCRIPTION:

We will discuss about symmetric encryption and visualization of Important cryptography concept:

1) Caeser Cipher
    a) Demonstration:
        i) https://en.wikipedia.org/wiki/Caesar_cipher
        ii) https://inventwithpython.com/cipherwheel/
        iii) https://md5decrypt.net/en/Caesar/#results
        iv) https://cryptii.com/pipes/caesar-cipher
        v) Encryption and decryption using RoT 13 in Mr Robot Decryption Scene https://www.youtube.com/watch?v=i9CBKGLVCME
    b) Character Frequency Count:
        i) http://xahlee.info/kbd/char_frequency_counter.html

2) Binary operation
    a) Ascii to hex conversion:
        i) http://www.ascii2hex.com/
    b) Xor calculator
        i) http://www.xor.pw/#
    c) XOR cipher

i) https://www.tutorialspoint.com/cryptography_with_python/cryptography_with_python_xor_process.htm
ii) https://www.abhishekshukla.com/python/adventures-in-cryptography-with-python-xor-cipher/
iii) https://samsclass.info/124/proj14/pxor.htm

d) Stream Cipher
i) https://pypi.org/project/pycrypto/
ii) https://pycryptodome.readthedocs.io/en/latest/src/cipher/cipher.html
iii) https://www.dlitz.net/software/pycrypto/api/current/

e) Symmetric Cipher (AES):
i) https://www.youtube.com/watch?v=gP4PqVGudtg

f) Symmetric cipher modes visualization in image
i) https://trustica.cz/en/2019/03/07/symmetric-cipher-modes/

g) Hashing
i) https://docs.python.org/2/library/hashlib.html
ii) https://riptutorial.com/python/topic/8710/sockets-and-message-encryption-decryption-between-client-and-server

h) Elliptic curve cryptography:
i) https://www.desmos.com/calculator/ute1r4um7g
ii) https://trustica.cz/en/category/ecc/

Symmetric encryption (AES) in Python:

```
from Crypto.Cipher import AES
obj = AES.new('This is a key123', AES.MODE_CBC, 'This is an IV456')
message = "The answer is no"
print(message)
ciphertext = obj.encrypt(message)
print("Encrypted Data",ciphertext)
```

```
obj2 = AES.new('This is a key123', AES.MODE_CBC, 'This is an IV456')
print("Decrypted Data", obj2.decrypt(ciphertext))
```